

Reclamation Manual

Policy

TEMPORARY RELEASE

(Expires 06/29/2011)

Subject:	Critical Cyber Asset (CCA) Security Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance
Purpose:	To establish specific organization requirements supporting compliance with the Critical Infrastructure Protection (CIP) Reliability Standards of NERC addressing the security of cyber systems supporting the Bulk Electric System (BES). The benefits of the Policy to the Bureau of Reclamation, its stakeholders, and the public are that compliance with the CIP Standards will help to minimize risks to the overall reliability of the BES. The BES is vital to the welfare of the nation as well as being essential for Reclamation to accomplish components of its mission.
Authority:	The Reclamation Act of 1902 (Act of June 17, 1902, ch. 1093, 32 Stat. 388), the Energy Policy Act of 1992 (Act of October 24, 1992, 106 Stat. 2776), the Flood Control Act of 1944 (Act of December 22, 1944, ch. 665, 58 Stat. 887), the Department of Energy Act of 1977 (Act of August 4, 1977, Pub. L. 95-91, 91 Stat. 565), acts relating to individual dams or projects, the Energy Policy Act of 2005 (Act of August 8, 2005, 119 Stat. 594), and Federal Energy Regulatory Commission (FERC) approved NERC Reliability Standards (18 CFR Part 40).
Approving Official:	Commissioner
Contact:	Director, Chief Information Office (CIO), 84-21000

1. **Introduction.** In recognition of its responsibilities to the public, and subject to other statute, Reclamation complies with applicable cyber security criteria, policies, practices, and standards as established under Federal legislation. This includes, but is not limited to, requirements outlined in Office of Management and Budget (OMB) Circular A-130 (Appendix III, as amended) and those contained in the Federal Information Security Management Act of 2002 (FISMA, 44 U.S.C. § 3541). The requirements identified in the aforementioned documents are applicable to all Reclamation cyber systems and are addressed in Reclamation's existing Information Technology Security Program and Policy (reference IRM P01, *Reclamation Information Technology Security Program*). Beginning with the passage of the Energy Policy Act of 2005 (Act), a number of new Federal cyber security requirements became effective. These requirements are directly applicable to a subset of Reclamation cyber systems referred to as CCAs where those cyber systems specifically support BES reliability. Under the provisions of the Act, all users, owners, and operators of such CCAs must comply with the cyber security requirements of the NERC CIP Reliability Standards.
 - A. This Policy directly supports the requirement, as established in the NERC CIP Reliability Standards, that responsible entities document and implement cyber security policy representing the commitment of management to secure its CCAs.

Reclamation Manual

Policy

TEMPORARY RELEASE

(Expires 06/29/2011)

- B. This Policy supplements overall Reliability Standard compliance requirements as outlined in Reclamation Policy, FAC P13, *North American Electric Reliability Corporation (NERC) Electric Reliability Standard Compliance*, and any related Directives and Standards (D&S). This Policy specifically addresses the NERC CIP cyber security objectives, roles, and responsibilities of Reclamation.
 - C. This Policy does not supersede Reclamation's existing Information Technology Security Program or Policy, as established in IRM P01; instead, it establishes supplemental security requirements specific to Reclamation cyber systems subject to protection requirements under the NERC CIP Reliability Standards.
2. **Applicability.** This Policy applies to all CCAs and related cyber-based assets supporting Reclamation power and attendant facilities operated and maintained directly by Reclamation staff. This Policy also applies to cyber systems and related cyber assets providing physical and/or logical protection for CCAs. Finally, all individuals (staff, contractors, and visitors) are subject to this Policy where those individuals have direct physical or logical access to CCAs or related cyber-based assets supporting Reclamation power and attendant facilities operated and maintained by Reclamation. All Reclamation offices involved in operating cyber systems with CCAs are required to implement this Policy within the limits imposed on Reclamation by Federal laws, orders, and regulations, including limitations on the expenditure of Federal funds.
3. **Definitions.**
- A. **Bulk Electric System.** As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition.
 - B. **Critical Assets.** Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the BES.
 - C. **Critical Cyber Assets.** Cyber Assets essential to the reliable operation of Critical Assets. This specifically includes computers, computer network components, and cyber-based peripheral and protective systems that are essential to the reliable operation of the BES.
 - D. **Directorate.** The organizational component of a Director. This includes the Director, Technical Resources; Regional Directors; Director, Security, Safety, and Law Enforcement (SSLE); Director, Policy and Administration; and Director, CIO.
 - E. **Directors.** Reclamation Senior Executives responsible for specific programs or facilities. This definition includes: the Director, Technical Resources; Regional Directors; Director, SSLE; Director, Policy and Administration; and Director, CIO.

Reclamation Manual

Policy

TEMPORARY RELEASE

(Expires 06/29/2011)

- F. **Regional Reliability Organization.** An entity that ensures that a defined area of the BES is reliable, adequate, and secure.
 - G. **Reliability Compliance.** The activities associated with meeting and maintaining adherence to the requirements listed in NERC CIP Reliability Standards or to cyber security related rulings by FERC relative to the reliability of the BES.
 - H. **Reliability Standards.** Any of a number of NERC or Western Electricity Coordinating Council (WECC) Standards families, the specific requirements of which are applicable to Reclamation, and which define tasks, procedures or conditions for maintaining the reliability of the BES. For purposes of this Policy, the specific Reliability Standards of concern include Standard CIP-002 through CIP-009, inclusive. Although CIP-001 is identifiable as a CIP Reliability Standard, it does not specifically address the Security of CCAs and is identified as outside the scope of this Policy. As used throughout this Policy, Standards CIP-002 through CIP-009 will be referred to collectively as the NERC CIP Reliability Standards.
 - I. **Senior Manager.** The Reclamation executive with overall responsibility and authority for leading and managing Reclamation's implementation of, and adherence to the NERC CIP Reliability Standards.
4. **Responsibilities.**
- A. **Commissioner.** The Commissioner has overall responsibility for compliance with all Reliability Standards.
 - B. **Deputy Commissioner for Operations.** The Deputy Commissioner for Operations provides executive leadership and directs compliance with Reliability Standards, including coordination of the Electric Reliability Compliance Program matters with the other Deputy Commissioners.
 - C. **Deputy Commissioner for Policy, Administration, and Budget.** The Deputy Commissioner for Policy, Administration, and Budget (PAB) shares executive leadership and compliance responsibilities with the Deputy Commissioner for Operations. As the executive level supervision for the Director, CIO, the Deputy Commissioner, PAB, provides resources as necessary to support and administer the CCA security efforts and this Policy.
 - D. **Director, Chief Information Office.** The Director, CIO is identified as Reclamation's Senior Manager with overall responsibility for leading and managing implementation and adherence to the NERC CIP Reliability Standards, CIP-002 through CIP-009, inclusive. The Director, CIO is also responsible for authorizing and documenting any necessary exceptions to requirements identified herein or in related D&S. Working with other responsible Directors and within the framework of the NERC CIP Reliability Standards, the Director, CIO, may delegate responsibilities for selected compliance activities to other

Reclamation Manual

Policy

TEMPORARY RELEASE

(Expires 06/29/2011)

Directorates in order to support overall compliance efforts. Such delegation shall be formally documented and accomplished with the concurrence of the parties involved.

- E. **Director, Technical Resources.** The Director, Technical Resources provides executive level supervision of the Senior Advisor, Hydropower and provides technical resources as required to administer Reclamation's overall Electric Reliability Compliance Program.
 - F. **Technical Resources, Senior Advisor, Hydropower.** The Senior Advisor, Hydropower administers the Electric Reliability Compliance Program. Working with all responsible Directors, the Senior Advisor, Hydropower, certifies compliance as applicable to NERC and WECC and advises the Deputy Commissioner for Operations on the status of Electric Reliability Compliance Program issues.
 - G. **Directors.** Each Director is responsible for the execution and documentation of all applicable NERC and WECC compliance activities, including the support and coordination of information technology related compliance requirements with the CIO. All such activities shall be focused on achieving, maintaining, and supporting demonstrable evidence of compliance with the Reliability Standards.
 - H. **Reliability Compliance Representative.** As required in Reclamation Manual Policy, *North American Electric Reliability Corporation (NERC) Electric Reliability Standard Compliance*, FAC P13, each Directorate is represented by a Reliability Compliance Representative who is responsible for coordinating Directorate compliance-related matters with the Power Resources Office and other Directorates.
 - I. **Area Managers.** Area managers are responsible for performing and documenting activities within the area office to maintain or become compliant with all Reliability Standards.
5. **Critical Cyber Asset Security Compliance.** Reclamation will administer and monitor the Cyber Security compliance of its CCAs and related cyber assets to ensure adherence with the NERC CIP Reliability Standards. The Director, CIO, may issue specific supplemental requirements as D&S to support this Policy.